UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/705,396	11/12/2003	Nadarajah Asokan	60091.00106	4400

32294 7590 06/06/2006

SQUIRE, SANDERS & DEMPSEY L.L.P.
14TH FLOOR
8000 TOWERS CRESCENT
TYSONS CORNER, VA 22182

EXAMINER	
D AGOSTA, STEPHEN M	

ART UNIT	PAPER NUMBER
2617	

DATE MAILED: 06/06/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/705,396	ASOKAN ET AL.	
	Examiner	Art Unit	
	Stephen M. D'Agosta	2617	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 May 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-31* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-31* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-2, 4, 6-8, 10-21 and 27-31 rejected under 35 U.S.C. 103(a) as being unpatentable over Tsuda and further in view of Kim.

As per **claims 1, 4, 6, 14, 21, 27-28 and 30,** Tsuda teaches a method for transmitting, to subscriber's user equipment, information required for a certificate issuance service in another network than a home network (see figure 10 shows mobile user registering with a foreign agent in a non-home network) in mobile communication system (title, abstract and figure 1 show a system that allows a user to be authenticated to roam to various networks and use services whereby AAA information is transmitted to/from a user's device), the method comprising: authenticating the subscriber (see figure 6, Step 2 and figure 10 which shows an authentication procedure); and transmitting to the user equipment at least part of the information required for obtaining the certificate in the other network (see figure 10) during the subscriber authentication (figure 10 shows overall procedure whereby data is sent to/from the mobile's AAA-H/AAA-V servers in order to authenticate said user as he roams. Figures 10-11 show mobile authenticating with AAA and P#186 discusses use of certificate issuance via certificate authority).

Tsuda also teaches a Mobile IP network (figure 1 shows a mobile user who has roamed from a home network #1001/#1010 to a visited network #1002/#1010 connected via IP which inherently subnets a network into smaller networks and their location is known based on where the engineer has positioned the local access

router/BTS). Further the mobile network maintains user location in an HLR and Tsuda teaches both home and foreign networks (P#67 and P#71) which inherently describes the concept of knowing where the user is since it is either in the (one) home network or in any of other foreign networks (see figure 18 which shows multiple foreign subnets, #1002/#1004);

But is silent on where the subscriber currently is located in a mobile communication system AND the method comprising: maintaining in the mobile communication system subscriber's location information and determining based of the subscriber's location.

Kim teaches "...FIG. 5 illustrates a base station system parameter database mounted on the home-zone service center 170. As shown in the drawing, the base station system parameter database stores every **base station's inherent ID (Bts_id), location information of each base station like latitude and longitude,** information about each sector like angle, system delay, and service range (angle, s_delay, svc_ran), exception range (exp_ran), change filed (change) and so forth. Before explaining about the exception range, it should be understood that the base stations located within the designated distance from the subscriber's residence regard (or decide) all sectors as a service sector. Here, the exception range is a value necessary for establishing the designated distance through which the base stations made the decision aforementioned...", (P#40) which shows that the location of each BTS is known (eg based on LAT/LONG) and would provide Tsuda with the location of the foreign agent/access router's location and hence, the location of the mobile unit it is communicating with.

With further regard to claims 1 and 4, Tsuda teaches a mobile user roaming (see figure 10) and requiring a connection between foreign and home AAA servers, which inherently will pass the address of the foreign node serving the mobile unit.

With further regard to claim 14, Tsuda teaches authentication via AAA servers (figure 10) for the purpose of roaming to other foreign networks and using services there, see figure 4 and P#69).

With further regard to claim 27, Tsuda teaches an authenticated channel via encryption (P#135).

It would have been obvious to one skilled in the art at the time of the invention to modify Tsuda, such that where the subscriber currently is located in a mobile communication system AND the method comprising: maintaining in the mobile communication system subscriber's location information and determining based of the

subscriber's location, to provide means for utilizing the user's location to assist with the authentication process to quickly identify which area the user has roamed to and what services may be available there.

As per **claim 2,** Tsuda teaches claim 1, further comprising: ~~receiving in the mobile communication system a message from subscriber's user equipment, the message indicating the address of the network node;~~ checking whether or not the address which the message indicated corresponds to the address determined on the basis of the location information; and if they do not correspond to each other, using the address determined on the basis of the location information (figure 1 shows a user roaming from network #1001 to network #1002, Mobile IP would inherently change the subnet address of the mobile unit to that of the Foreign Agent since the user has roamed to a new access point).

As per **claim 7,** Tsuda teaches claim 6, wherein the authentication is application level authentication (figure 10 shows the process by which the user's authentication "program" communicates with other AAA server programs for authentication. Also se figure 11 and figures 12a-d which show packet layout. Hence the examiner interprets Tsuda's design as the AAA process being an application level authentication since it "rides on top of" the Mobile IP layer).

As per **claim 8,** Tsuda teaches claim 6, wherein the service is ~~certificate issuance service and~~ the user equipment utilizes said part of the information during a certificate issuance procedure in a visited network (figures 10-11 show mobile authenticating with AAA and P#186 discusses use of certificate issuance via certificate authority).

As per **claims 10 and 16,** Tsuda teaches claim 6/15, wherein said part of the information comprises at least an address of a network node via which the service is provided (figure 1 shows the user roaming from home Mobile IP subnet to another Mobile IP subnet whereby the network node address of the home agent #1011 and foreign agents #1021 would be ascertained as the unit roams).

As per **claims 11 and 18,** Tsuda teaches claim 6/14, wherein said part of the information comprises at least a public key required for the service (P#186).

As per **claim 12,** Tsuda teaches claim 6, wherein said part of the information comprises at least an indication of the protocol required for the service (Tsuda teaches using the Mobile IP protocol. Figures 12a-d show the packet layout).

As per **claim 13,** Tsuda teaches claim 6, wherein the service is certificate issuance service and said part of the information comprises at least an address of a network node via which the service is provided and the method further comprising transmitting from the user equipment a certificate request to the network node (figure 10 shows the overall authentication from the mobile user #1010 to visited and home AAA servers via the Foreign Agent. Certificate issuance is supported by Tsuda, see P#186).

As per **claim 15,** Tsuda teaches claim 14, wherein the message and the reply message are transmitted in an integrity protected channel (P#135).

As per **claim 17,** Tsuda teaches claim 16, further comprising transmitting from the user equipment a certificate request to the network node (P#186).

As per **claim 19,** Tsuda teaches claim 15, wherein said part of the information comprises at least an indication of the protocol required for the service (Tsuda teaches Mobile IP and packet layouts, see figures 12a-d. IP Headers inherently use a field to indicate the type of protocol and service).

As per **claim 20,** Tsuda teaches claim 11, wherein the message relates to a certificate issuance service (P#186).

As per **claim 29,** Tsuda teaches claim 28, wherein the ~~network node (AU-H) is in a home network and the~~ other network node is in a visited network (figure 1 shows a home network #1001 and visited/foreign network #1002).

As per **claim 31,** Tsuda teaches claim 30, wherein the user equipment (UE) is arranged to receive said part of the information from a network node with which the user equipment was authenticated, the network node being in a home network (figure 10 shows authentication as user roams whereby the process includes links from mobile to foreign agent, to AAA-F, to AAA-H concluding at the Home Agent, whereby the AAA-H and home agent can be interpreted as network nodes in the home network).

Claims 3-5, 9, 22-23 and 25 rejected under 35 U.S.C. 103(a) as being unpatentable over Tsuda/Kim and further in view of Sandhu et al. US 2002/0145561.

As per **claim 3,** Tsuda teaches claim 1, further comprising: ~~receiving in the mobile communication system a message from subscriber's user equipment,~~ checking whether or not the location information in the message corresponds to the location information maintained in the system; and using the maintained location information if it does not correspond to the location information in the message (figure 1 shows a user in either a Home Network #1001 whereby the user communicates with the home agent #1011 and/or the user roaming to a Visited/Foreign network #1002 and communicates with the Foreign agent #1021. Either means would inherently include the network understanding where the user is located based on the IP Address of the IP Subnet for the Access Point) **but is silent on** location information.

Kim teaches determining location of the mobile user based on the BTS's LAT/LONG being known and hence a mobile communicating with a specific BTS will inherently have it's location determined (P#40).

Sandhu teaches "A method and system whereby two mobile units can locate each other is presented. A user connects an interface device, such as a personal digital assistance (PDA), a wireless phone, a laptop, or a pager, to a mobile unit. The mobile unit regularly obtains its location through a location-determining technology (e.g., GPS) and sends the location to a service provider computer. The service provider computer maintains a database of the current location of all the mobile units, and provides the location of mobile units to each of the mobile units." (Abstract).

It would have been obvious to one skilled in the art at the time of the invention to modify Tsuda, such that location information is used, to provide means for utilizing the user's location to assist with the authentication process to quickly identify which area the user has roamed to and what services may be available there.

As per **claim 5,** Tsuda teaches claim 4 **but is silent on** wherein the message contains a global cell identifier which indicates the subscriber's location information.

Kim teaches "FIG. 5 illustrates a base station system parameter database mounted on the home-zone service center 170. As shown in the drawing, the base station system parameter database stores every **base station's inherent ID (Bts_id), location information of each base station like latitude and longitude,** information about each sector like angle, system delay, and service range (angle, s_delay, svc_ran), exception range (exp_ran), change filed (change) and so forth." (P#40). The examiner interprets the BTS-ID as being the Global Cell-ID.

It would have been obvious to one skilled in the art at the time of the invention to modify Tsuda, such that the message contains a global cell identifier which indicates the subscriber's location information, to provide means for utilizing the user's location to assist with the authentication process to quickly identify which area the user has roamed to and what services may be available there.

As per **claim 9,** Tsuda teaches claim 6 **but is silent on** wherein said part of the information is location network specific information.

Tsuda teaches an elaborate process whereby a user can authenticate with foreign/home AAA servers for services as they roam (see figures 10-11).

Kim teaches "...FIG. 5 illustrates a base station system parameter database mounted on the home-zone service center 170. As shown in the drawing, the base station system parameter database stores every **base station's inherent ID (Bts id), location information of each base station like latitude and longitude,..**". (P#40) which shows that the location of each BTS is known (eg based on LAT/LONG) and would provide Tsuda with the location of the foreign agent/access router's location and hence, the location of the mobile unit it is communicating with.

Sandhu teaches "A method and system whereby two mobile units can locate each other is presented. The mobile unit regularly obtains its location through a location-determining technology (e.g., GPS) and sends the location to a service provider computer. The service provider computer maintains a database of the current location of all the mobile units, and provides the location of mobile units to each of the mobile units." (Abstract).
It would have been obvious to one skilled in the art at the time of the invention to modify Tsuda, such that said part of the information is location network specific information, to provide means for the system to understand where the mobile unit is located and provide services as requested by the user for that location and charge accordingly.

As per **claim 22,** Tsuda teaches claim 21, wherein the location network is a visited network (figure 1 shows home network #1001 and visited network #1002).

As per **claim 23,** Tsuda teaches claim 21 comprising a gateway network for certificate requests in a home network of the user equipment, the gateway network being configured to perform the network node address determination (figures 1 and 10 show the operation for a roaming mobile IP user to access home/foreign networks and access network nodes/gateways (eg. access points/routers, or agents) whereby mobile

IP will provide the address of said network node/gateway. Tsuda teaches using certificates from a certificate authority - paragraph P#186).

As per **claim 25,** Tsuda teaches claim 1, further comprising: ~~receiving in the mobile communication system a message from subscriber's user equipment,~~ checking whether or not the location information in the message corresponds to the location information maintained in the system; and using the maintained location information if it does not correspond to the location information in the message (figure 1 shows a user in either a Home Network #1001 whereby the user communicates with the home agent #1011 and/or the user roaming to a Visited/Foreign network #1002 and communicates with the Foreign agent #1021. Either means would inherently include the network understanding where the user is located based on the IP Address of the IP Subnet for the Access Point) **but is silent on** location information.

Kim teaches determining location of the mobile user based on the BTS's LAT/LONG being known and hence a mobile communicating with a specific BTS will inherently have it's location determined (P#40).

Sandhu teaches "A method and system whereby two mobile units can locate each other is presented. A user connects an interface device, such as a personal digital assistance (PDA), a wireless phone, a laptop, or a pager, to a mobile unit. The mobile unit regularly obtains its location through a location-determining technology (e.g., GPS) and sends the location to a service provider computer. The service provider computer maintains a database of the current location of all the mobile units, and provides the location of mobile units to each of the mobile units." (Abstract).

It would have been obvious to one skilled in the art at the time of the invention to modify Tsuda, such that location information is used, to provide means for utilizing the user's location to assist with the authentication process to quickly identify (or send error

message as to) which area the user has roamed to and what services may be available there.

Claims 24 and 26 rejected under 35 U.S.C. 103(a) as being unpatentable over Tsuda/Kim/Sandhu and further in view of Okazaki et al. US 2003/0092425.

As per **claim 24,** Tsuda teaches claim 1, further comprising: ~~receiving in the mobile communication system a message from subscriber's user equipment~~ and checking whether or not the location information in the message corresponds to the location information maintained in the system (figure 1 shows a user in either a Home Network #1001 whereby the user communicates with the home agent #1011 and/or the user roaming to a Visited/Foreign network #1002 and communicates with the Foreign agent #1021. Either means would inherently include the network understanding where the user is located based on the IP Address of the IP Subnet for the Access Point) **but is silent on** the message including subscriber's location information; and if it does not correspond to the location information in the message, sending an error indication by using the maintained location information.

Kim teaches determining location of the mobile user based on the BTS's LAT/LONG being known and hence a mobile communicating with a specific BTS will inherently have it's location determined (P#40).

Sandhu teaches "A method and system whereby two mobile units can locate each other is presented. The mobile unit regularly obtains its location through a location-determining technology (e.g., GPS) and sends the location to a service provider computer. The service provider computer maintains a database of the current location of all the mobile units, and provides the location of mobile units to each of the mobile units." (Abstract).

Okazaki teaches securing access in a mobile IP network (title) that uses AAA authentication whereby error messages are used [P#53] "...MN then sends a registration request (MIP_Reg_Request) to FA2 (Step 71). This request includes MN's home address, the address of MN's home agent (HA) and MN's identification, such as its Network

Access Identifier (NAI). FA2 formats the request into Diameter messages and sends the formatted registration request to the local administrative server AAA_FA1 (Step 72). Upon receiving the request from FA2, AAA_FA1 determines the home administrative server of MN and forwards the request to AAA_HA (Step 73). AAA_HA performs the identity verification of MN. If AAA_HA fails to verify the identity of MN, it returns an error message to AAA_FA1. If, however, AAA_HA successfully verifies the identity of MN, AAA_HA then sends the request to HA (Step 74)..". Okazaki's use of error-handling reads on the claim.

It would have been obvious to one skilled in the art at the time of the invention to modify Tsuda, such that the message including subscriber's location information; and if it does not correspond to the location information in the message, sending an error indication by using the maintained location information, to provide means for utilizing the user's location to assist with the authentication process to quickly identify (or send error message as to) which area the user has roamed to and what services may be available there.

As per **claim 26,** Tsuda teaches claim 1, further comprising: ~~receiving in the mobile communication system a message from subscriber's user equipment,~~ (figure 1 shows a user in either a Home Network #1001 whereby the user communicates with the home agent #1011 and/or the user roaming to a Visited/Foreign network #1002 and communicates with the Foreign agent #1021. Either means would inherently include the network understanding where the user is located based on the IP Address of the IP Subnet for the Access Point) **but is silent on** checking whether or not the location information in the message corresponds to the location information maintained in the system; and if it does not correspond to the maintained location information, sending an error indication by using the location information in the message and location information.

Kim teaches determining location of the mobile user based on the BTS's LAT/LONG being known and hence a mobile communicating with a specific BTS will inherently have it's location determined (P#40).

Sandhu teaches "A method and system whereby two mobile units can locate each other is presented. A user connects an interface device, such as a personal digital assistance (PDA), a wireless phone, a laptop, or a pager, to a mobile unit. The mobile unit regularly obtains its location through a location-determining technology (e.g., GPS) and sends the location to a service provider computer. The service provider computer maintains a database of the current location of all the mobile units, and provides the location of mobile units to each of the mobile units." (Abstract).

Okazaki teaches securing access in a mobile IP network (title) that uses AAA authentication whereby error messages are used [P#53] "...MN then sends a registration request (MIP_Reg_Request) to FA2 (Step 71). This request includes MN's home address, the address of MN's home agent (HA) and MN's identification, such as its Network Access Identifier (NAI). FA2 formats the request into Diameter messages and sends the formatted registration request to the local administrative server AAA_FA1 (Step 72). Upon receiving the request from FA2, AAA_FA1 determines the home administrative server of MN and forwards the request to AAA_HA (Step 73). AAA_HA performs the identity verification of MN. If AAA_HA fails to verify the identity of MN, it returns an error message to AAA_FA1. If, however, AAA_HA successfully verifies the identity of MN, AAA_HA then sends the request to HA (Step 74)..". Okazaki's use of error-handling reads on the claim.

It would have been obvious to one skilled in the art at the time of the invention to modify Tsuda, such that it checks whether or not the location information in the message corresponds to the location information maintained in the system; and if it does not correspond to the maintained location information, sending an error indication by using the location information in the message, to provide means for utilizing the user's location to assist with the authentication process to quickly identify (or send error message as to) which area the user has roamed to and what services may be available there.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Stephen M. D'Agosta whose telephone number is 571-272-7862. The examiner can normally be reached on M-F, 8am to 5pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Bill Trost can be reached on 571-272-7872. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

STEVE M. D'AGOSTA
PRIMARY EXAMINER

5-30-06